John A. Carey
Inspector General

OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

Inspector General
Accredited

"Enhancing Public Trust in Government"

Redacted per §119.0725(2)(b)

Audit Report

2024-A-0003

Village of Wellington - IT Application Security Audit

March 27, 2024

OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

AUDIT REPORT
2024-A-0003

DATE ISSUED: MARCH 27, 2024

John A. Carey
Inspector General

Inspector General
Accredited

"Enhancing Public Trust in Government"

VILLAGE OF WELLINGTON - IT APPLICATION SECURITY AUDIT

SUMMARY

WHAT WE DID

We conducted an audit of the Village of Wellington's (Village) Information Technology (IT) Application Security. This audit was performed as part of the Office of Inspector General (OIG), Palm Beach County 2022 Audit Plan.

Our audit focused on IT application accounts, records and related activities from October 1, 2018 to October 25, 2022.

WHAT WE FOUND

Overall, we found that 1) application user access and administrative privileges were managed effectively to prevent unauthorized access and maintain sufficient separation of duties, 2) administrative privileges were controlled and application access was based on roles and job duties, and 3) application accounts were managed effectively and in compliance with applicable licensing agreements. However, we found a weakness related to the disabling of user accounts upon employee separation for two (2) IT applications.

The Village did not always disable separated users' access in a timely manner

We found the Village did not always disable separated users' access in a timely manner.

The Village's IT policies and procedures do not establish a time period in which departments must notify IT of employee separations or for disabling inactive application user accounts.

Without timely removal of access to Village applications, there is an increased risk of unauthorized access and modification to data such as personnel timekeeping records, or [redacted]

WHAT WE RECOMMEND

Our report contains one (1) finding and two (2) recommendations. Implementation of the recommendations will assist the Village in strengthening application user access controls and help ensure compliance with the Village's New Hire & Separation IT/Software Assignments Procedure.

The Village concurred and accepted our recommendations.

We have included the Village's management response as Attachment 1.

BACKGROUND

The Village was incorporated on December 31, 1995. The Charter of the Village was enacted by the Laws of Florida in the year of incorporation. The Village is located in western Palm Beach County and shares a southwestern boundary with the Florida Everglades. The Village's population in 2021 was estimated to be 61,768.

The Village operates under the council-manager form of government. The Village Council consists of five (5) Village councilmembers, one of whom is the Mayor, who are elected at-large on a nonpartisan basis. The Mayor acts as head of the Village for service of process, ceremonial matters, and the signature of ordinances, contracts, deeds, bonds, and other instruments and documents. The Village Manager is the chief administrative officer of the Village. Day to day affairs of the Village are under the leadership of the Village Manager, who is appointed by the Council.

The OIG 2022 Annual Audit Plan included IT Application Security audits. We selected the Village for audit because it operates a water utility, which increases the Village's IT application security risk, and because it had not been audited by the OIG since 2012.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objectives of the audit were to determine whether:

- Application user access was managed effectively to prevent unauthorized access and maintain sufficient separation of duties;
- Administrative privileges were controlled and user access was based on roles and job duties; and
- Application accounts were managed effectively and in compliance with applicable licensing agreements.

The scope of the audit included, but was not limited to, IT Application security records and activities for the period October 1, 2018 to October 25, 2022.

The audit methodology included but was not limited to:

- Review of ordinances, policies, procedures, contracts, agreements, and related requirements;
- Completion of process walk-throughs;
- Review of internal controls related to account management and user access for Village IT applications;
- Interview of appropriate personnel;
- Review of records, logs, and reports; and
- Performing detailed testing of selected IT application accounts and users' access.

This audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient,

appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDING AND RECOMMENDATIONS

Finding (1): The Village did not always disable separated users' access in a timely manner.

Section 218.33, Florida Statutes (2019), states,

> (3) Each local government entity shall establish and maintain internal controls designed to:
>
> (a) Prevent and detect fraud, waste, and abuse as defined in s. 11.45(1).
>
> (b) Promote and encourage compliance with applicable laws, rules, contracts, grant agreements, and best practices.
>
> (c) Support economical and efficient operations.
>
> (d) Ensure reliability of financial records and reports.
>
> (e) Safeguard assets.

The National Institute of Standards and Technology[1] (NIST) created a cybersecurity risk framework for use by critical infrastructure owners and operators. The NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Framework) Core consists of five interrelated functions:

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Each function of the Framework is sub-divided into categories of cybersecurity outcomes closely tied to programmatic needs and particular activities. Each category is further

[1] As part of the U.S. Department of Commerce, NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. The State of Florida Cybersecurity Standards are modeled after the NIST Framework and the Federal Information Security Management Act of 2002. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Additionally, as of July 1, 2022, Section 282.3185, Florida Statutes requires municipalities to adopt cybersecurity standards consistent with generally accepted best practices for cybersecurity, including National Institute of Standards and Technology Cybersecurity Framework based on their population. The Village's effective date was January 1, 2024.

divided into subcategories of specific outcomes of technical and/or management activities. Each subcategory references specific standards, guidelines, and practices that can be used to achieve the subcategory's outcomes.

Under the "Protect" function is the category "Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions." Under the category PR.AC is the subcategory "PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes." Subcategory PR.AC-1 references NIST Special Publication 800-53 AC-2.

The NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations states,

> **AC-2 ACCOUNT MANAGEMENT**
>
> Control:
>
> ...
>
> f. Create, enable, modify, disable, and remove accounts in accordance with [*Assignment: organization-defined policy, procedures, prerequisites, and criteria*];
>
> ...
>
> Control Enhancements:
>
> ...
>
> (3) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS
>
> **Disable accounts with [*Assignment: organization-defined time period*] when the accounts:**
> **(a) Have expired;**
> **(b) Are no longer associated with a user or individual;**
> **(c) Are in violation of organizational policy; or**
> **(d) Have been inactive for [*Assignment: organization-defined time period*]."**
>
> Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

The Village's New Hire & Separation IT/Software Assignments Procedure, effective August 12, 2022, states,

> 3) Procedures
> a) Candidate Hiring Approval

...

iii) Separation Notification

(1) HR must open a support ticket with IT (support@wellingtonfl.gov) to remove all access and reclaim any hardware.

(2) Upon receipt of a support ticket requesting IT Software/Hardware Assignments, the IT Department reviews the request applies the correct separation checklist:

(a) This includes but is not limited to turning off any and all IT assigned access to: door control access, remote desktop access, software logins, [redacted] login, ERP access, identify and reclaim hardware, etc.

(b) Once separation checklist is completed. IT will close the ticket. Doing so will notify the owner of the ticket as well as anyone that was added as a cc on the ticket.

(3) The VOW department Head must make sure to turn off/remove/disable any access to 3rd party software(s)/website(s) that are not controlled by IT (for example but not limited to the following: [redacted] Fingerprint software/hardware, etc.).

We selected eleven (11) Village applications for testing based on their importance to the overall functioning of the Village. The following applications were selected:

Application
Cyber Security Software
Timekeeping Software
Recruitment Software
Permitting Software
Network Monitoring Software
Utilities Meter Software
Air Conditioning Control Software
Point of Sale Software
Human Resources Software
ERP Software
Utilities Software

We selected a sample of 38 user accounts whose access had been disabled from six (6)[2] Village applications to determine if the Village properly disabled the users' access in a timely manner.

[2] Five (5) of the eleven (11) applications selected did not have any disabled user accounts during the audit period.

Of the 38 user accounts tested, we found the Village:

- Disabled one (1) user's account for the timekeeping software[3] 38 days after the employee's separation from Village employment, and
- Disabled eight (8) users' accounts[4] for the Utilities software between 8 and 473 days after separation from Village employment. See chart below for details:

User	Application	Separation Date	# of Days to Disable Account after Separation
User 1	Utilities Software	2/23/2022	8
User 2	Utilities Software	4/30/2022	11
User 3	Utilities Software	2/27/2020	20
User 4	Utilities Software	4/2/2020	32
User 5	Utilities Software	1/7/2020	32
User 6	Timekeeping Software	1/15/2022	38
User 7	Utilities Software	5/6/2022	133
User 8	Utilities Software	12/30/2020	428
User 9	Utilities Software	11/15/2020	473

The Human Resources department notified the IT department of User 6's separation of employment from the Village 38 days after the effective date of the separation. As a result, the user's access to the timekeeping software was disabled 38 days after the former employee had any legitimate basis for accessing the timekeeping software. The Village informed us that this employee was part time, did not have a set number of hours or days that he worked, and did not inform his supervisor of his decision to resign in a timely manner.

The IT department disabled the access control system[5] accounts and removed badge access for the eight (8) utilities software application users within 3 days of the employee's separation from the Village; however, the Utilities Department did not disable the users' utilities software accounts in a timely manner.[6] Although the utilities software application can only be accessed on the Village network using an enabled access control system account, [redacted]

[3] We used the date that the employee's access control system account was disabled because the Village's timekeeping software authenticates users using the access control system's credentials via the single sign-on process.
[4] One (1) user had two (2) accounts in the utilities software for separate modules of the application.
[5] The access control system stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information. Security is integrated with the access control system through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network.
[6] The utilities software is a third party application controlled by the Utilities department.

The Village stated that the disabling of the employees' access control system accounts and badge access, along with the Information Technology Policies requirement prohibiting the sharing of passwords[7] helps to mitigate the risk of unauthorized access. While the policy requirement is effective in establishing management's expectation for authorized use of Village applications, the action of removing all logical access to Village applications upon an employee's separation provides the most assurance in preventing unauthorized access.

Additionally, the Village's Information Technology Policies (v2.4) and the New Hire & Separation IT/Software Assignments Procedure do not establish a time period in which departments must notify IT of employee separations or for disabling inactive application user accounts.

Without timely removal of access to Village applications, there is an increased risk of unauthorized access and modification to data, such as personnel timekeeping records, or [redacted] Although the risk to the utilities software is minimal, there is an unnecessary vulnerability wherein critical system information could be accessed and altered by unauthorized persons.

Recommendations:

(1) The Village update its policies and procedures to include a defined time frame to notify IT of employee separations and for disabling inactive application user accounts.

(2) The Village ensure staff are aware of their roles and responsibilities related to notifying IT of employee separations and for disabling inactive application user accounts.

Management Responses:

(1) The Village concurs with recommendation #1. The Policies and procedure have been updated to include defined time frames as presented.

(2) The Village concurs with recommendation #2. Staff completes certifications for mandatory review of Information Technology Policies upon hiring, and on an annual basis or when policies are updated (ongoing).

[7] Version 2.4, effective October 15, 2020, Password Policy section 3.2.2 Password Protection Standards states "Do not share Village of Wellington passwords with anyone, including administrative assistants or secretaries." and "All passwords are to be treated as sensitive, confidential Village of Wellington information."

ACKNOWLEDGEMENT

The Inspector General's audit staff would like to extend our appreciation to the Village of Wellington's staff for their assistance and support in the completion of this audit.

This report is available on the OIG website at: http://www.pbcgov.com/OIG. Please address inquiries regarding this report to the Director of Audit by email at inspector@pbc.gov or by telephone at (561) 233-2350.

ATTACHMENT

Attachment 1 – Village of Wellington's Management Response

ATTACHMENT 1 – VILLAGE OF WELLINGTON'S MANAGEMENT RESPONSE

Attachment 1 – Village of Wellington's Management Response

The Village concurs with recommendation #1. The Policies and procedure have been updated to include defined time frames as presented.

The Village concurs with recommendation #2. Staff completes certifications for mandatory review of Information Technology Policies upon hiring, and on an annual basis or when the policies are updated (ongoing).